A framework for authentication in NBD tactical Ad Hoc Networks

A. M. Hegland, E. Winjum , O.-E. Hedenstad

***Abstract*—Network–based Defense (NBD) and the all-IP network make authentication ever more important. But a generally accepted and comprehensive authentication suite lacks. This work is a step towards filling the gap. The article proposes a three-level framework for authentication in NBD tactical ad hoc networks. Hop-by-hop network level authentication provides the basic protection. End-to-end application level authentication is included only when finer resolution is needed. The third level of authentication relates to physical node access.**

The framework may serve as a reference for authentication also in other networks. An additional contribution is the approach used to derive the authentication framework, which has general relevance.

***Index Terms*—Authentication, Security, IP, ad hoc networks**

I. Introduction

Authentication refers to the verification of identities. The identity is proven through something which the entity *is*, *has*, or *knows*. Typical examples are fingerprints, cryptographic keys and passwords. It is usually used in conjunction with authorization and access control. The entity to be authenticated can be a software application, a hardware device or a person or other.

In NBD, information shall be available where needed and whenever needed. NBD enables communication between a large numbers of nodes at different levels in the command hierarchy and across previously separate network domains. This enhances the need for proper authentication.

Authentication is also a basic building block in the protected core network (PCN) concept described by Hallingstad and Oudkerk [1]. The protected core is a transport network that connects colored clouds. The colored clouds are plaintext networks where users connect. They are separated from the PCN by IPsec encryption devices. Access control is enforced on all connections. The PCN only includes authenticated nodes. This hop-by-hop authentication prevents external attackers from flooding the protected transport network.

Whereas NBD applies to a wider scope, the article puts emphasis on a network centric operational scenario of tactical ad hoc networks. Extending the NBD concept from strategic networks to the lower echelons of tactical networks with limited bandwidth, varying network connectivity and often resource constrained nodes, makes authentication even more difficult. The dismounted soldier level is also more prone to node capture.

Despite the fact that authentication has become more important, a comprehensive and commonly adopted authentication framework still does not exist. Few standards and scientific publications focus on authentication at the lower tactical echelons. FIPS PUB 140-2[2] describes requirements for authentication of the operator at log-on. It specifies authentication at the granularity of roles or individual identities depending on chosen security level. Authentication mechanisms specified in IETF RFCs to a large extent focus on network access, assuming a fixed network infrastructure. Once the user or machine has proven its identity, he or it is allowed to transmit and receive information over this network.

On this background, the article proposes a three-level framework for authentication in tactical ad hoc networks. The framework can be adopted as is, but a main intention is also to serve as a reference model for the discussion of authentication in NBD and other networks.

Another contribution is the approach used to derive the authentication framework. It has general relevance, and is not limited to the scope of tactical ad hoc networks.

We start with definitions and terms in Section II. Then the scenario and basic authentication challenge is studied in section III. Section IV elaborates on identities that are candidate for authentication. Section V defines the trust and threat models. Requirements are then defined in section VI, before the framework for authentication at multiple levels is proposed in Section VII. Its compliance with the requirements is discussed in section VIII. Related work is described in section IX. The concluding remarks and further work are summarized in section X.

II. Definitions

This article distinguishes between the following types of authentication: *entity authentication*, *data origin authentication (message authentication)*, *transaction authentication* and *key authentication* [3].

Entity authentication refers to the traditional two or three step protocol where the supplicant convinces the authenticator that he is currently communicating with the identity claimed

A. M. Hegland is with Kongsberg Defence & Aerospace, Billingstad, Norway; e-mail: anne.marie.hegland@ kongsberg.com.

E. Winjum is with the Norwegian Defence Research Establishment, Kjeller, Norway, e-mail: eli.winjum@ffi.no.

O.-E. Hedenstad is with the Norwegian Defence Research Establishment, Kjeller, Norway, e-mail: ole-erik.hedenstad@ffi.no.

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2011.6035819

by the supplicant. Then the protocol terminates. The *authenticator* controls access to a protected resource. The *supplicant* tries to get access by being authenticated by the authenticator through an authentication protocol.

The terms *supplicant* and *authenticator* are usually used for entity authentication. We here extend their use to other types of authentication to help clarify which end verifies what. It is always the identity of the supplicant that is authenticated.

Data origin authentication (message authentication) assures the receiver (authenticator) that the message at some point in time originated from the claimed source (supplicant). The two main effects of data origin authentication are verification of the originator and verification of the binding between the originator and the content – including integrity protection of the message content.

Transaction authentication is parallel to data origin authentication, but includes time-variant parameters that enable the receivers to detect the timeliness of the message. This makes replay detection possible.

Key authentication is what is achieved through the validation of a public key certificate; the authenticator is convinced that a key belongs to specific party. The digital signature of the issuing certificate authority (CA) guarantees the authenticity of the binding between the identity of the key owner and the public key. The authenticator verifies the identity of the third party which signed the certificate. Key authentication does not necessarily involve any actions from the key owner.

Data origin authentication, transaction authentication and key authentication are *unilateral ("one-way").* Entity authentication can also be *mutual ("two-way").*

Identity and identifiers: The *identity* (ID) specifies a unique entity, for instance a user, a role, an application or a host. The identity is represented by one or more *identifiers* – for instance a number or a text string.

In general, a *user* has an identity tied to a single entity [4]. An entity can also be a *group* of entities referred to by a single identifier. In tactical networks it is often more important to authenticate an entity as a valid group member (friend or foe) rather than tracking the specific group member. The members of the group must be distinguishable, but the set has an identity separate from its elements. A role provides certain rights – typically access rights. Other entities in our scenario include hosts and processes/applications.

A **Security domain** is defined as a collection of entities to which applies a single security policy enforced by a single authority [2].

Trusted bindings: Our authentication framework relies on a trusted computing base (TCB) that enables trusted bindings between identities. Trusted binding means that if an identity *A* have a trusted binding to identity *B* and this identity (B) is authenticated, then identity A need not be authenticated. The article assumes a TCB implemented in a *trusted communication node* that has been certified in accordance with given security and assurance criteria.

III. Scenario and basic authentication challenge

A. Tactical Ad Hoc Network

Figure 1 illustrates our scenario: Secure information sharing over a coalition tactical army group mobile ad hoc network (MANET). Vehicles as well as dismounted soldiers carry wireless communications nodes that form the MANET. Basic services includes amongst other voice and position reports. Most of the communication has only short term value.

The MANET connects to a fixed or deployable infrastructure, but connectivity cannot be guaranteed at all times. The types of nodes, resource constraints and network connectivity vary.

The MANET differs from a true ad hoc network in the sense that it has a planned origin and only authorized nodes are included in the network. The security requirements are stricter than in most civilian ad hoc network applications. The users have differing roles and access rights. For simplicity, the article assumes a single security domain and one classification level.

Local information exchange takes place within physical proximity of the trusted communication node over a short range connection. It includes *system access data* exchanged between the communication node and a local user, and data sent to or from a local peripheral. It also includes communication between different processes *inside* the communication node (not illustrated).

Remote information exchange refers to communication between nodes that are one or more hops away, and requires a running network service. It includes management data as well as voice and other user data.

B. The basic authentication challenge

Figure 2 illustrates the basic authentication challenge; *verification of identities of trusted entities communicating in a non-trusted environment that includes entities with different access rights and varying trustworthiness, and where one or more of the trusted entities controls access to a protected resource.*

The model is generic. The protected resource can be an application, a routing table or other part of memory, a peripheral or other.

The trusted entities are communication nodes communicating over a wireless channel, applications inside the communication node or a user communicating with a trusted communication node. Note that the *environment* in Figure 2 refers not only to the wireless channel, but also to the operating system, applications with different access rights, and users with various privileges. The figure also applies for multiple security levels and different security domains.

If the trusted entities were all in an environment where all had the same access rights, all behaved according to the protocols and non-repudiation was not required; authentication would be superfluous.

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2011.6035819

The wireless communication channel and battery powered terminals reduce the assortment of usable authentication mechanisms, but the basic challenge remains.

IV. Identities

A large number of identities and corresponding identifiers are involved from the system powers up until a message is exchanged. As an example a node decides its own *host name*. Then a number of processes are launched – each is identified with a *process id*. Identifiers are also combined into new identifiers, for instance *sockets* consisting of source and destination IP-addresses and port numbers. Table 1 illustrates the diversity. It is not exhaustive, but shows that a large number of identities are candidates for authentication.

V. Threat and trust models

The proper authentication depends on the threat and trust models that apply for the studied scenario.

Threat model: The Dolev-Yao threat model [5] assumes an active external intruder that can read, modify and redirect all messages, but not decrypt or forge a signature without the correct cryptographic key. The Dolev-Yao threat model is here adopted with the addition that the threat can also originate from an insider with legal physical access to the communication nodes, but who tries to access applications other than those she is authorized to access.

Trust model: Coalition partners are assumed to trust each other to follow the agreed security policy and service level agreements. They are trusted to forward traffic on the other party's behalf even if they are not authorized to access the contents of the payload. Only trusted communication nodes are included in the ad hoc network.

VI. Requirements for authentication in NBD

A. General requirements

Security: A main requirement is that the authentication scheme must not reduce system availability. Authorized users must get access when required. The communicating parties must be able to verify the identity of the other party at the granularity required for the type of information exchanged. Unauthorized users and nodes must not gain access to network resources and protected data.

Resource consumption: The wireless channel requires a bandwidth efficient authentication scheme, and battery powered nodes necessitate energy efficient mechanisms.

Robustness: The authentication protocol must be simple and robust to link-losses. It must be possible to exclude one or more nodes and still communicate securely with the remaining partners.

Human intervention: Human intervention for entering authentication credentials is only acceptable in the preparatory phase prior to the operation.

B. Requirements related to information type

Table 2 outlines authentication requirements related to the different types of information exchange of our scenario. It distinguishes between the two main categories: local and remote information exchange. Local relates to local system access. Remote includes all information exchange that takes place over the network between two or more communication nodes. In addition to user data, this includes both remote system access (log-on over the network) and management data. The latter refers to security management data, QoS signaling as well as other network management traffic such as routing information.

The next columns specify type of authentication required (None, Entity, Transaction, Data origin or Key Authentication) and granularity needed (authentication at the level of individuals or group member). The table also indicates whether one-way (Unilateral) or two-ways (Mutual) authentication is needed, and the types of identities involved (Host, Application User or role). The authentication level column refers to the three-level authentication framework presented in the next section.

The intention of the table is to provide a condensed overview. Although the table can be simplified for a specific case, it illustrates the complexity. To summarize:

Local information exchange requires entity authentication –if any. The local environment is to a large extent controllable. Though, special peripherals, such as those containing security configuration data, may necessitate mutual authentication.

Remote information exchange needs the whole range of authentication mechanisms. The specific needs depend on the type of information and situation/security policy.

Remote log-on and on-line management require mutual entity authentication. Otherwise the parties cannot be sure who is in the opposite end. Key authentication is necessary where certificate-based public key scheme are used.

Unilateral transaction authentication is the basis for push-based user - and management data. For instance, unilateral authentication of routing messages enables differentiation between authorized and unauthorized members of the network. Transaction authentication is preferred over message authentication where resilience to replay and other DoS attacks are important. Critical data such as shooting orders may justify additional measures. Data originating from higher levels in the command hierarchy typically demand authentication at a finer granularity than data flowing from lower levels and upwards.

VII. A Three-level authentication framework

Identities that cross the borders of the trusted communication node are either related to node access information exchange between local entities, or communicated over the network end-to-end between applications or hop-by-hop. This leads to the three-level authentication framework illustrated in Figure 3.

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2011.6035819

Within each of the three authentication levels we distinguish between authentication at the granularity of individuals (single entities) and the more coarse grain group member. In most cases, verifying role and rank in the command hierarchy is more important than tracking the specific individual. Authentication is either unilateral or mutual. See also the rightmost column of Table 2.

Node access level refers to the entity authentication of a user that logs on to the local node or remote application. It also includes entity authentication of peripheral equipment connecting to the communication node. Human intervention is needed. Node access level authentication is generally not time-critical.

The identities involved represent users, users in specific roles and equipment.

Application level refers to end-to-end authentication between local and remote applications as well as local authentication between internal applications. It also includes authentication of stored objects. The identities involved are application identities. Human voice recognition is considered a special case of application level authentication.

Network level refers to hop-by-hop authentication at the IP or lower levels of the protocol stack. The identities involved are related to the network service, and typical identifiers include network and link layer addresses. No human intervention is needed. Whereas the application level authentication can assume an already running (authenticated) network service, the network level cannot. Network level authentication is also referred to as *basic* authentication. Each datagram or segment is authenticated separately.

A. Use of the three levels

Network level authentication: Unilateral network level authentication provided hop-by-hop at the link layer or by the network layer using a group key is here suggested as basic authentication.

Traditionally, wireless military communication systems include cryptographic confidentiality protection at the link-layer. Unless the security policy states something else, the implicit authentication achieved through the possession of the correct key, can be used to authenticate the peer as a valid member of the network. Proper encryption and decryption of the message shows that the sending and receiving party possesses the correct key.

The term *basic* authentication refers to the fact that all datagrams receive this protection. It reduces the need for additional authentication at the application level.

Time information, such as sequence numbers or time stamps, is required to achieve *transaction* authentication. Depending on whether IPsec or link-layer protection is used, we assume any sequence number or initialization vector included in the IP-packet or MAC layer frame is exploited as timing information to achieve transaction authentication.

In our scenario we assume all coalition partners share the same network level authentication key. This enables the formation of a trusted coalition ad hoc network and authenticated exchange of “basic” user data such as position reports. Coalition partners that move into the area are automatically included in the trusted network and start receiving position reports with the aid of the network level authentication key.

However, whereas all nodes in the network are trusted to forward data on the others’ behalf and exchange position data, additional end-to-end authentication is required for other types of data. One example is shooting orders.

Application level authentication: Application level end-to-end authentication is only added when higher granularity is needed.

Different authentication mechanisms integrated with each application increase the complexity and imply more cryptographic keys. An end-to-end authentication mechanism which is common to more applications scales better. The Transport Layer Security (TLS) protocol [6] and Secure Shell (SSH) [7] intended for secure remote log-in and are two options. IPsec [8] is another. Application level authentication enforced at the network layer by IPsec requires security associations which discriminate between different applications.

IPsec may be used both for application level authentication and network level authentication, e.g. an “inner” IPsec tunnel provides end-to-end authentication at the application level, and an “outer” authenticates data hop-by-hop at the network level using a group key.

Node access level authentication is primarily a question of entity authentication. For scenarios which demand high availability, the users can be authenticated in multiple ways at local log-on. The basic services such as voice must be easily available. A pin code or password is the typical approach. Multiple factors are suggested for access to more security-critical applications and remote log-on.

For access to the basic services, we assume the authentication lasts for the entire tactical operation. Access to more advanced services may call for re-authentication.

Local peripherals will be under the control of the operator. When the operator is logged-in, new peripherals such as sensors can be added without additional authentication of the device. Wireless peripherals and security critical peripherals such as media carrying cryptographic keys must still be authenticated. The authentication can be based on a pre-shared symmetric key, delayed disclosure of values in a hash chain or public keys.

B. Authentication mechanisms

The authentication mechanisms are all founded on one of two basic pre-conditions: a *pre-shared secret* such as a password or cryptographic key, or a *non-secret pattern received through an authenticated channel.* An example of the latter is the certificate authority’s public key that enables verification of certificates. Another example is a biometric data that enables later recognition of its owner.

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2011.6035819

Entity authentication mechanisms: Passwords are the typical solution. A drawback is their tendency to be low-entropy. Other mechanisms for unilateral entity authentication include biometric methods, tokens and combinations of more factors. Tokens can carry longer passwords or cryptographic keys and certificates. Biometric methods provide high granularity. But high sensitivity makes them prone to false denials. False positives are also a problem. Under threat neither passwords nor biometric methods and tokens prevent misuse.

Mutual entity authentication of devices necessitates pre-shared keys, certificates or combinations of schemes.

There is no single entity authentication mechanism that is clearly superior to the other approaches for tactical use. The simplest solution is passwords - possibly combined with tokens.

Key authentication mechanisms: are needed when public key schemes are used. The public keys are authenticated through certificates. X.509 is the commonly adopted standard. The authenticator must both verify the certificate authority's signature on the certificate, and check that the certificate has not been revoked. The revocation methods for fixed networks are generally not very well suited for the ad hoc environment. Some, such as *online certificate status protocol* (OCSP) [9], require guaranteed connectivity to a central trusted entity to check certificate validity status on-line. Others trade update cost for timeliness or vice versa. The well known *certificate revocation list* (CRL) usually include all revocations within the security domain, and is typically updated weekly or every second week.

The bandwidth consumption of certificate exchanges and revocation information limit the applicability of public key schemes in tactical ad hoc networks. Schemes not depending on the availability of a single certificate authority are sought.

Data origin and Transaction authentication are achieved through a symmetric integrity check value or digital signature appended to each message.

Digital signatures enable non-repudiation and authentication at the granularity of individuals, and can be verified both hop-by-hop and end-to-end. But the overhead is significant. A digital signature and certificate typically add 2kilobits or more. Appending this to each datagram or link layer MAC segment would exhaust the wireless media. Altogether, digital signatures are unsuited for message and transaction authentication at the network level.

Symmetric methods do not support non-repudiation. Authentication at the granularity of individuals necessitates different keys for each user. This scales badly. Still, symmetric integrity check values are more efficient than digital signatures in the sense that they are shorter and computationally less expensive. And bandwidth consuming certificate exchange and validation are avoided. By using a group key symmetric schemes are well suited for verification of group memberships.

Identity-based signature schemes [10] provide the benefits of digital signatures without certificates. The identity serves as public key. The corresponding private key is derived by a trusted authority. The computational complexity and signature sizes are comparable to digital signatures. Identity-based schemes have not gained widespread use so far, but represent an interesting alternative to certificate-based public key schemes.

VIII. FULFILLMENT OF THE REQUIREMENTS

The three-level framework is tailored to the requirements related to information type. The choice of authentication mechanism decides its special characteristics as illustrated in Table 2. The general requirements are met in the following way:

Security: The proposed scheme rests on the assumptions of trusted communication nodes.

Related to the threat model; the node access level authentication enables separation of roles and prevents that insiders in possession of the equipment gain unauthorized access.

The basic network level authentication prevents external attackers from being included in the network. It distinguishes between group members and non-group members and enforce access control hop-by-hop. The application level authentication enables further differentiation. The end-to-end authentication prevents intermediate (insider) nodes from undetectably introducing information they are not authorized to on the behalf of others.

Even if application level end-to-end authentication is included, network level authentication is still needed in addition to make it possible for the intermediate nodes to decide whether the datagram comes from an authorized member or not before they forward it.

Resource consumption: Basic network level authentication based on symmetric keys limits the computational complexity and reduces the bandwidth consumption compared to public key approaches. And the two-tiered approach where application level authentication is only included for specific applications also contributes to this. To what extent network level authentication at the link-layer or at the IP-layer performs better, depends to some extent on the implementation. IPsec is in general known to introduce more overhead than link-level mechanisms.

Human intervention: The proposed scheme requires pre-shared secrets or authenticated patterns. It is assumed that the initial keys are distributed in the preparatory phase prior to the operation. Whereas user level authentication requires human intervention, application level and network level authentication do not.

IX. RELATED WORK

Candolin, Lundber and Kari [11] propose the *packet level authentication* (PLA) scheme as a generic security solution for military ad hoc networks. PLA assumes each IP-datagram is digitally signed by its originator. The IPv6 extension header

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2011.6035819

carries both the signature and the corresponding public key certificate. This enables all nodes to authenticate any datagram.

The PLA scheme represents one way to implement the basic network level authentication proposed here. But the inclusion of digital signatures and certificates in every datagram represent a significant overhead. Reference [11] does not consider bandwidth consumption. The bandwidth consumption significantly limits the applicability of PLA in wireless environments.

The framework presented in this article has parallels to the security framework for service oriented architectures proposed by Candolin[12]. In contrast to this article, Candolin focuses on confidentiality and distinguishes between content security, communication security and network security. The content level protects the contents such as information and services both in store and in transit. Communication level provides end-to-end security between nodes. Network security is concerned with protecting the network infrastructure and includes services such as access control and denial-of service protection.

X. Concluding remarks and Further work

The proposed authentication framework maps well with the PCN concept. The next hop node is authenticated at the network level. The authentication framework with multiple levels can thus be used as a building-block in the implementation of a PCN.

The framework for authentication focuses on wireless communication between trusted communications nodes. The discussions also apply for a host or network wired to the node. Depending on whether the host and communication node resides within the same controlled area, they regard each other as remote nodes or local peripherals.

The trusted communication node can be generalized to trusted components. Identities inside the trusted communication nodes and trusted components have a *trusted binding* in the sense that they co-exist in the same trusted environment. The trusted communication nodes or components are trusted to obey the security policy, and any attempts to introduce a false identity or otherwise jeopardize the security, will be detected and prevented. Authentication is required when an identifier leaves the trusted communication node and enters a non-trusted environment. But if the identifier is encapsulated by -or linked to- another identifier that is authenticated by the same peer trusted communication node, it need not be authenticated separately. Trusted communication nodes and trusted components are subjects for further work.

A coalition of multiple nations will likely include more security domains and possibly several security levels. This does not alter the basic authentication problems that need to be solved. But the separation achieved through trusted communication nodes will no longer be enough to enable proper trusted bindings. Trusted components inside the trusted communication node or similar will be required in addition. Furthermore, there are both political and technical problems to be solved. And there must be a way of filtering and translation between comparable classification levels if information is to be transferred from one domain to another. Different domains may use different identities. Authentication with multi-level security systems and multiple security domains are topics for further work.

Traditional security solutions assume one network represent one security domain and one classification level. This assumption does not easily map with the future network based defense with a mixture of security domains and classification levels and schemes within one single network. The network must convey information of multiple classification levels. Data can be carried over different links depending on trust requirements as described in [13] and [14].

The article focuses on data in transit. Data at rest demands authentication credentials stored with the object, or included in a way that enables authentication also at a later time. An example is situational pictures that are stored after reception. Authentication of stored objects is an additional topic for further work.

References

[1] G. Hallingstad, and S. Oudkerk, “Protected Core Networking: An Architectural Approach to Secure and Flexible Communication,” *IEEE Communications Magazine*, vol. 6, no. 11, Nov. 2008, pp. 35-41.

[2] National Institute of Standards and Technology (NIST), “Security Requirements for Cryptographic Modules” FIPS PUB 140-2, Jan. 1994, with change notes 12-03-2002.

[3] A.J. Menezes, P.C.v.Oorschot, and S.A. Vanstone, “Handbook of Applied Cryptography,”*CRC press*, 1997.

[4] M. Bishop, “Computer Security, Art and Science,” *Addison Wesley*, 2003, p. 355.

[5] D. Dolev, and A. Yao, “On the security of public key protocols,” *IEEE Transactions on Information Theory*, vol. 29, no. 2, Mar. 1983, pp. 198-208.

[6] T. Dierks, and E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.2,” *IETF*, RFC 5246, Aug. 2008.

[7] T. Ylonen, and C. Lonvick, Ed.,”The Secure Shell (SSH) Protocol Architecture,” *IETF* RFC 4251, Jan. 2006.

[8] S. Kent, and K. Seo, “Security Architecture for the Internet Protocol,” (IPsec), *IETF* RFC 4301, Dec. 2005.

[9] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, “X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol – OSCP,” *IETF* RFC 2560, Jun. 1999.

[10] A. Shamir, “Identity-based crypto systems and signature schemes,” *CRYPTO’84*, 1984.

[11] C. Candolin, J. Lundber, and H. Kari, “Packet level authentication in military networks,” In *Proceedings of the 6th Australian Information Warfare & IT Security Conference*, Geelong, Australia, Nov. 2005.

[12] C. Candolin, “A Security Framework for Service oriented Architectures,”In *Proceedings of IEEE MILCOM*, 2007.

[13] E. Winjum, and B. K. Mølmann, “A multidimensjonal approach to multilevel security,” *Information Management & Computer Security*, vol. 16, no. 5, 2008, pp. 436-447.

[14] E. Winjum, “Trust metric routing in ad hoc networks,” *PhD Dissertation*, University of Oslo, 2006.

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2011.6035819

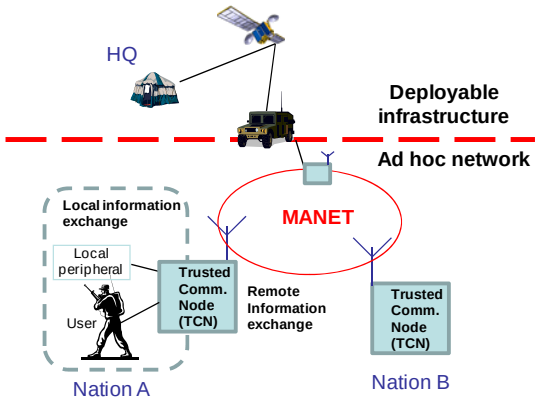

Figure 1 Scenario: Tactical Army Group Ad Hoc Network

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2011.6035819

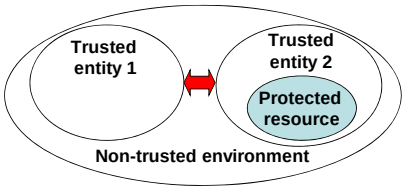

Figure 2 The basic authentication challenge

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2011.6035819

Table 1 The diversity of identities and identifiers

Identity	Identifiers
User-related	User name, Log-on name, Group name, Role
Hardware-related	Hardware device ID, Host name
Application-related	
Operating system	Name, Process IDs
Software module	Issuer name, version, "Code Digest"
DNS server	Domain name, host name, IP address
SIP: User Agent, registrar, redirect server, invitee, proxy server	SIP address (SIP URI), IP address
RTP source	RTP SSRC, RTP CSRC
	Session ID
Router	Name, Router IDs
Other applications	other application specific IDs
Communication layers	
Transport	Port number, Socket, Session ID
IP	IP address, Flow ID, Protocol ID, Sequence number, DSCP value, ECN bits
MAC	MAC address, MAC priority
PHY	Preamble, Coding scheme, Frequency hopping key
Security application IDs	
Certificate owner, Certificate authority, CRL distribution point	Certificate number, CA name, Name of certificate owner, Algorithm IDs
Security Association	SPI, Key reference

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2011.6035819

Table 2 Authentication matrix for different types of information exchange

Information exchange			Auth. type	Granu-larity	Unilateral / Mutual	Identities	Authenti-cation level
Local	System access	Local processes	N/A	N/A	N/A	(Appl)	Node access
		Local peripheral	E or N/A	In or N/A	Mut or N/A	Host/Appl	
		Local Operator Log-on	E	In or Gr	Uni	User/Role	
Remote		Remote Log-on	E	In or Gr	Mut	User/Role/Appl	
	Manage-ment data	Network management	E, T/D	In or Gr	Mut or Uni	User/Role/Appl	Application or Network level
		QoS signalling	E, T/D	In or Gr	Mut or Uni	User/Role/Appl	
		Security management	E, K, T/D	In or Gr	Mut or Uni	User/Role/Appl	
	User data	Situational picture,Orders, Alarms from higher level	T/D	In	Uni	Role/Host/Appl	Application
		Sensor data, Alarms from lower level, Logistics & Status reports	T/D	In or Gr	Uni	Role/Host/Appl	Application or Network level
		Voice	E	In or Gr	Mut or Uni	Role	
		Position Reports	T/D	Gr	Uni	Role/Host/Appl	Network level
		Short messages	T/D	Gr	Uni	Role/Appl	

N/A= Not Applicable/None
E = Entity Authentication
K = Key Authentication
T = Transaction Authentication
D = Data origin Authentication

In = Individual
Gr = Group

Mut= Mutual
Uni = Unilateral

Appl= Application (refers to specific process)
User = Specific operator
Role = User in specific role
Host = Communication node or hardware device

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2011.6035819

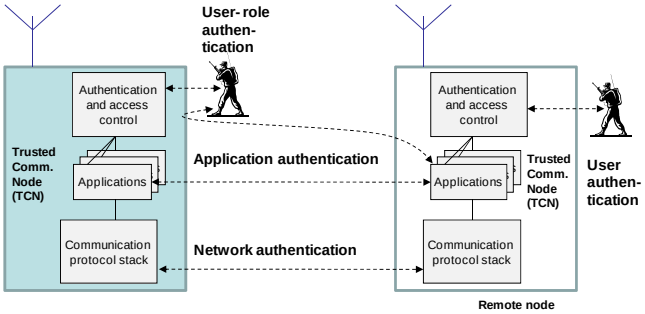

Figure 3 Authentication levels

Dette er en postprint-versjon / This is a postprint version.
DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2011.6035819

Biographies

Anne Marie Hegland is a Senior Systems Engineer at Kongsberg Defence & Aerospace, Norway. She received her MSc in electronics from the Norwegian University of Science and Technology in 1997, and a PhD in informatics from the University of Oslo in 2007. She has many years of experience in the fields of communications and crypto systems. Her current research interests include QoS, internet protocols, information security and ad hoc networks.

Eli Winjum is a Director of Research at the Norwegian Defence Research Establishment (FFI). She received her MSc in coding theory from the University of Bergen and her PhD in communications systems from the University of Oslo. Before joining FFI, she was within public telecommunications operations and management for several years. Her current research interests include information security, secure routing and mobile wireless ad hoc networks.

Ole-Erik Hedenstad is a chief scientist at the Norwegian Defence Research Establishment (FFI). He received his MSc in computer science from the Norwegian University of Science and Technology. He has many years of experience in the fields of command and control information systems, and military message handling systems. His current research interests include information security and service oriented architectures.

DOI til publisert versjon / DOI to published version: 10.1109/MCOM.2011.6035819